US 20040064736A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2004/0064736 A1

Obrecht et al.

(43) Pub. Date: Apr. 1, 2004

# (54) METHOD AND APPARATUS FOR DETECTING MALICIOUS CODE IN AN INFORMATION HANDLING SYSTEM

(75) Inventors: **Mark Eric Obrecht**, Austin, TX (US); **Michael Anthony Alagna**, Austin, TX (US); **Charles Andrew Payne**, Austin, TX (US)

Correspondence Address:
**HAYNES AND BOONE, LLP**
**901 MAIN STREET, SUITE 3100**
**DALLAS, TX 75202 (US)**

(73) Assignee: **WholeSecurity, Inc.**, Austin, TX

(21) Appl. No.: **10/647,644**

(22) Filed: **Aug. 25, 2003**

**Related U.S. Application Data**

(63) Continuation-in-part of application No. 10/231,557, filed on Aug. 30, 2002.

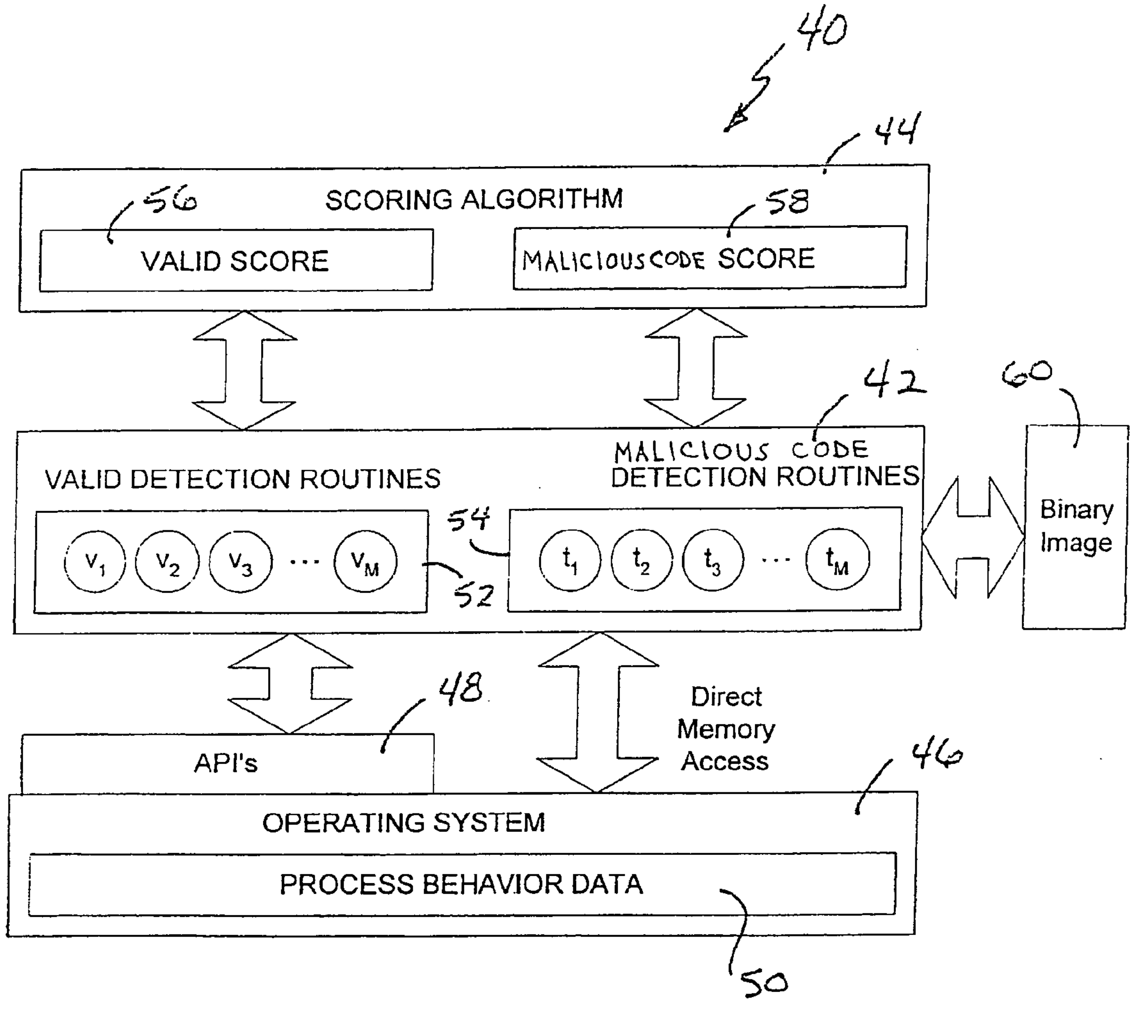
**Publication Classification**

(51) **Int. Cl.**$^{7}$ .......... **G06F 11/30**

(52) **U.S. Cl.** .......... **713/201**

## (57) ABSTRACT

Malicious code detection code is executed by an information handling system. The malicious code detection code includes detection routines. The detection routines are applied to executable code under investigation. The detection routines associate weights to respective code under investigation in response to detections of a valid program or malicious code as a function of the detection routines. It is determined whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.


40
44
SCORING ALGORITHM
56
58
VALID SCORE
MALICIOUSCODE SCORE
42
60
VALID DETECTION ROUTINES
MALICIOUS CODE DETECTION ROUTINES
$V_1$
$V_2$
$V_3$
...
$V_M$
54
52
$t_1$
$t_2$
$t_3$
...
$t_M$
Binary Image
48
Direct Memory Access
API's
46
OPERATING SYSTEM
PROCESS BEHAVIOR DATA
50